Attachment A

June 18, 2012

Chief Judge Mark L. Wolf
U.S. District Court
Moakley U.S. Courthouse
Boston, MA 02210

Dear Chief Judge Wolf:

I currently serve as Sr. Director of Enterprise Security at Charter Communications. I helped start the Internet Security team at Charter in 2001. I am submitting this Victim Impact Statement on behalf of Charter to help explain the damage that Mr. Harris has caused.

Most people think of cable theft as a minor crime. However, the consequences of Mr. Harris's actions were far worse than just giving individuals a chance to surf the Internet without paying for it.

For Charter, as a company, there were financial damages estimated at several hundred thousand dollars in lost revenue -- based on the number of cable modems that Mr. Harris sold to customers in Charter's service area. These modems had been modified to allow the purchaser to receive unauthorized Internet service. And Mr. Harris also sold thousands of these "modified modems" to customers in other parts of the country. So the actual amount of lost revenue across the industry is estimated to be at least $3.8 million.

What we know for sure is that cloned modems impact the service of paying customers using the Internet. Charter, like all cable companies, sizes the infrastructure of their networks to provide reliable speeds for the anticipated customers. As more subscribers are added, we upgrade the equipment in proportion to the customer growth. However, as a result, cloned cable modems on a piece of the network slowed down the service for other, paying customers. And if Mr. Harris's customer was using a cloned modem with the same identity as a paying customer, near the same geographic location, the paying customer could lose their Internet connection completely.

I work in Charter's corporate headquarters in St. Louis and have daily contact with Charter staff across the country. I first became acquainted with TCN-ISO, Mr. Harris's website, as early as 2004. I was very surprised that he was able to advertize hacked modems so openly. I had frequent conversations with engineers in the field who alerted me to the site. We held regular brainstorming sessions on how to secure the network from these modems.

Charter Plaza ◦ 12405 Powerscourt Drive ◦ St. Louis, Missouri ◦ 63131-3674
www.charter.com ◦ tel: 314.965.0555 ◦ fax: 314.965.9491

As Benjamin Brodfuhrer testified during the trial, our Corporate Engineering Team purchased hacked modems ourselves from TCN-ISO to use for developing a defense against this. In my experience, TCN-ISO was the always the predominate website for purchasing hacked cable modems. I'm sure that there were a few cloned modems purchased from other sites. But, the only site I was worried about was TCN-ISO. As I remember, it was the easiest to find in an Internet search.

At some stage in the research, an engineer in our corporate office was able to develop a program that would scan our entire network looking for duplicate modems. My team was responsible for testing the program. We found that the first version of it was very good at identifying duplicate modem MAC numbers, but it didn't do a good job of distinguishing the legitimate user from the individuals who were using a cloned version of the modem for unauthorized access.

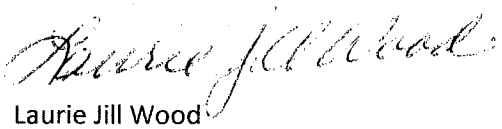
I felt strongly that we didn't want any authorized customers to be negatively impacted by our cloned modem remediation activities. Therefore, we didn't remove any modems from the network until we had researched the databases and logs to be absolutely sure that it was a clone and not the legitimate customer. And, the manual labor involved with trying to determine the legitimate customer was often so burdensome that it was cost-prohibitive.

After a couple more years of research, our engineers and developers were able to come up with a system that would not only identify duplicate modems, like those sold by TCN-ISO, but also correctly distinguish the legitimate customer. We were able to develop automation that would successfully integrate into our billing and provisioning systems so that that the anti-cloning system would automatically disable connectivity for the cloned modems. The development time for this process took several years. I'm proud of Charter's engineers because Charter was one of the first major cable companies to develop this capability. Later other companies asked if we would share our code.

Far worse than the financial damage to Charter are consequences related to assistance Mr. Harris's methods may have given to criminals wanting to conceal their identity on the Internet. Until the industry was able to invent and implement processes to interfere with network access for these modems, anonymity was provided for the user. Law enforcement was able to subpoena and review access logs, but the criminal's actions were completely untraceable from the logs. Certainly, the information and modems sold by Mr. Harris' company were used by many of his customers to steal our service and degrade the performance of the network for paying customers. But they may have also been used by criminals to help conceal their identity or evade law enforcement. Mr. Harris is a very smart, successful entrepreneur. However, the information and equipment he sold was always used to commit crimes. And, in some cases, terrible crimes.

I ask that you bear that in mind in your sentencing. Thank you.

Sincerely,



Laurie Jill Wood
Sr. Dir., Enterprise Security